AMENDMENTS TO THE SPECIFICATION:

Please replace paragraph 24 with the following amended paragraph:

[24] As shown in Fig. 1, in some embodiments credential authority 102 supplies its certification requirements 103 to an application developer 106 and a certification service 104. Application developer 106 creates an application 107a ~~in~~ that conforms to requirements 103 and provides it to certification service 104. Certification service analyzes and tests application 107a to make sure that it meets the requirements 103 specified by credential authority 102. An application 107a that satisfies these requirements is given an appropriate credential or certificate 105. Upon obtaining credential 105, the application developer 106 may distribute the credentialed application 107 to an application user 108.

Please replace paragraphs 29 and 30, with the following amended paragraphs:

[029] In some embodiments the user's system 108 includes digital rights management hardware and/or software for managing protected content and for enforcing the rules and controls associated therewith. For example, InterTrust's INTERRIGHTS POINT™ ~~InterRights Point™~~ software or RIGHTS/SYSTEM™ ~~Rights/System™~~ software could be used, as could the Rights Operating System software described in the '900 patent or other systems that implement some or all of the virtual distribution environment functionality described therein. Alternatively, other digital rights management hardware and/or software could be used. Use of digital rights management software/hardware may be helpful in situations where the user may not be

trusted and/or where the user's system may be deemed to be otherwise insufficiently secure or reliable. As explained in the '900 patent, digital rights management software/hardware can be used to ensure the secure, confidential, and reliable performance of important operations, such as enforcing the rules associated with content (e.g., making sure that a credential check is performed, and that it is performed accurately).

[030] In preferred embodiments, communications between the user 108 and the content provider 101 and/or content packager 110 are conducted via secure containers (e.g., encrypted electronic files). For example, DIGIBOX® ~~DigiBox®~~ or DIGIFILE™ ~~DigiFile™~~ secure containers produced by InterTrust Technologies Corporation of 955 Stewart Drive, Sunnyvale ~~4750 Patrick Henry Drive, Santa Clara~~, California could be used. When a user attempts to access content contained in a secure container, the user's application sends the content to the digital rights management system which extracts the content and/or the rules associated with the content, evaluates the rules, and determines whether the application is allowed to access the content and on what terms access should occur. For example, the digital rights management system preferably handles the credential-verification process described above, and releases content to a rendering application only if the appropriate credential is found and verified.